Models of critical information infrastructure protection

Dan Assaf

University of Toronto, Faculty of Law, 84 Queen’s Park, Toronto, ON M5S 2C5, Canada

Abstract

This paper advocates the need to conceptualize or model critical information infrastructure protection (CIIP) in order to explain regulatory choices made by governments regarding CIIP. Building on previous attempts, it proposes two models of CIIP: the national security model and the business continuity model. Each of these models is based on a different, sometimes contrasting, set of values, namely, security values and neo-liberal values. As the choice of regulatory mechanism is dependent on the manner in which CIIP is perceived by governments, an analysis is essential to assess and understand national CIIP policies. A comparative analysis of American and Israeli policies is conducted to clarify the major issues regarding CIIP and to provide a basis for proposing CIIP models.

1. Introduction

The problem of providing adequate CIIP is similar to public problems that states encounter and, thus, requires remedy by government through intervention or through facilitation of private sector remedies [15]. Governments may employ a variety of institutional arrangements to ensure that adequate CIIP is provided. These arrangements are characterized by varying degrees of intervention, from pure state provision of CIIP, through collaborative arrangements between the public and private sectors, to pure market provision of CIIP.

The government’s perception of CIIP has significant policy implications in terms of the choice of regulatory mechanism. Hence, the conceptualization or modeling of CIIP is vital when attempting to assess and explain different CIIP policies. Different models are important for placing national policies in their wider social and political contexts, and for identifying the sets of values that generate them.

This paper attempts to conceptualize or model CIIP and identify the values inherent in the concepts/models. A comparative analysis of American and Israeli policies is conducted to frame the major issues related to CIIP and to provide a basis for proposing CIIP models.

2. Regulatory continuum

Government intervention in CIIP may range from pure state provision of CIIP, through collaborative arrangements between the public and private sectors, to pure market provision of CIIP (where, in theory, government has no role). Fig. 1 presents the regulatory continuum. The most interventionist option lies at the left end of the continuum (Point A): governments opt for “in house” provision of CIIP through government ownership of assets. The “command and control” regulation lies slightly to the right (B) in the continuum. In this case, the state mandates clear and precise cyber security standards through legislation or other statutory instruments, and monitors and enforces
Fig. 1 – Regulatory continuum.

these standards via criminal laws with penalties ranging from fines to prison terms. Thus, in this highly interventionist mode, the state dictates to the private sector exactly how CIIs are to be protected.

More to the right (C) is a mode where rule-making powers are delegated to public agencies; these agencies have discretionary powers to set standards, monitor and enforce compliance. The rationale is that a regulatory agency would have more expertise and its independence would insulate it from political influence. The degree of intervention, as in the “command and control” arrangement, is relatively high.

Points A–C are characterized by high degrees of intervention by the state in the market — rule-making powers, monitoring and enforcement responsibilities are assumed by the state, and the role of the private sector is limited to compliance with regulatory requirements. The next set of points in the continuum is distinguished by a mixture of public and private collaboration in rule-making, monitoring and enforcement.

Point D represents a situation where the state, through a public agency, engages in consultation, perhaps even negotiation, with regulated entities. Thus, direct regulations are tailored to individual firms or trade associations, who agree to work with the government to achieve common goals. While the state retains its discretionary power, it seeks greater acceptance (and hence compliance) from the market.

Point E, which denotes enforced self-regulation, represents a conceptual change where the state’s role shifts from being prescriptive to facilitative (although some coercion may be involved). In this paradigm, approaches based on risk, process, management and performance confer the role of rule-making on the private sector with some oversight or ratification by government entities [5]. For example, a legislature could empower a regulatory agency to compel a company or trade association to write cyber security rules that address the contingencies facing that entity. The agency would then ratify and approve the rules. Enforcement would be done internally with minimal intervention on the part of the agency. However, the agency could privatize one of its roles – either rule-making or enforcement – leaving the government with more discretion.

Voluntary self-regulation (F) is the next point in the continuum. In this setting, standards are developed and enforced privately without (or with very little) government involvement. Compliance with standards is expected as a matter of good practice. In many cases, self-regulation is performed by existing trade associations that can require their members to comply with the standards [4].

The last point of interest (G) is the market. The underlying idea is that the market will adjust and reach socially-optimal objectives on its own. The role of the government is limited to encouraging and inducing market transactions. In the context of CIIP, consumers might be willing to pay more for reliable electricity provision and resilience to cyber attacks. In this case, profit incentives induce private firms to invest in cyber security. Competition would then drive all electricity providers to invest in such measures. The government would merely provide a stable legal framework for market transactions.

3. Contrasting approaches

The United States and Israel provide good test cases for a discussion on CIIP regulation since they are similar in some respects, yet very different in others. Both countries share a perceived higher threat and risk related to national security and homeland security. In addition, both countries are technologically-advanced and rely heavily on information systems in every aspect of society. Consequently, CIIP is an important component of their national security and homeland security policies.

Nevertheless, the United States and Israel are very different in their choice of regulatory arrangements regarding CIIP. While the US mainly employs market-based mechanisms to provide CIIP, Israel has adopted a state-centric, interventionist approach that relies on its security apparatus to regulate CIIP. Interestingly, despite the similarity of the perceived threat and technological development in the two countries, neo-classical economic ideology appears to play a more dominant role than security values in promulgating national security and homeland security policies in the United States than in Israel and vice versa.

3.1. United States

The origins of American CIIP policy date to the mid 1990s. The awareness of the terrorist threat to critical infrastructures was largely the result of the World Trade Center and Oklahoma City bombings in 1993 and 1995, respectively [12]. From its inception, the leitmotif of American CIIP policy has been that government should refrain from
intervening in the market, and instead seek voluntary cooperation from private owners and operators of critical infrastructures (who are responsible for approximately 85% of the nation’s critical infrastructure assets). By relying on market mechanisms to motivate private actors to take protective actions, improve infrastructure resilience and share information about vulnerabilities, threats and risks, the US Government has essentially chosen a “hands off” approach [12–14,17].

The main objective of US CIIP policy has been to “[p]romote a partnership between government and infrastructure owners and operators beginning with increased sharing of information relating to infrastructure threats, vulnerabilities, and interdependencies” [17]. Regulation was not an option. Instead, attempts were made to promote voluntary self-regulation by industry sectors and establish private-public partnerships for information sharing [6].

The responsibility for developing CIIP standards (e.g., for security administration and management, electronic perimeter security, access control, awareness and training, and incident response and recovery plans) was left to the private sector. This was done mainly through existing self-regulatory trade associations and by governmental endorsement of Information Sharing and Analysis Centers (ISACs) and other public-private partnerships. The rationale – in terms of regulatory policy-making – was that this would foster voluntary self-regulation by industry. The government sought to play a very limited role, one that required it, at most, to foster private institutions that would set up cyber security standards.

Two exceptions to the US policy of non-intervention in CIIP have occurred in the chemical and energy sectors. In the case of the chemical sector, section 550 of the Homeland Security Appropriations Act of 2007 [21] mandated federal standards (including cyber security regulations) for securing high-risk chemical facilities. The act authorized the Department of Homeland Security (DHS) to promulgate “interim final regulations” to assure the security of high-risk chemical facilities. On April 2007, DHS issued an interim final rule (effective June 8, 2007) that established risk-based performance standards and required thousands of chemical facilities that use or store significant quantities of toxic chemicals to perform vulnerability assessments and take steps to secure their facilities.

In the case of the energy sector, the Federal Energy Regulatory Commission (FERC) is currently in the process of approving a number of cyber security standards developed by the North-American Electric Reliability Corporation (NERC), an energy sector trade association. The US Congress authorized this regulatory activity via the Energy Policy Act of 2005. This led FERC to certify NERC as an electric reliability organization (ERO) with the mission to develop and enforce (subject to FERC approval) mandatory reliability standards (including cyber security rules) for bulk power systems.

It comes as no surprise that the chemical and energy sectors are the first to see deviations from the US Government’s hands off CIIP policy. The chemical sector is a hazardous sector per se — the risk associated with a cyber attack on a chemical facility is very clear. The consequences of the 2003 blackout in the Northeastern US and Canada underscore the importance of the energy infrastructure. Thus, direct regulation in the chemical sector and enforced self-regulation sanctioned by the government in the energy sector have been introduced as more intervening regulatory tools. Despite these interventions, US CIIP policy is largely driven by hostility to government intervention.

3.2. Israel

The CIIP regulatory arrangements in Israel sharply contrast with those of the United States [3]. The Israeli policy can be characterized as state-centric and interventionist, with law and hierarchical control as its cornerstones.

In 2000, recognizing the threat posed by information operations on critical infrastructure assets, the Israeli security community worked on drafting a CIIP policy. The main debate centered on which organization should have an overall responsibility for CIIP [3]. The CIIP plan was approved by the Israeli Government in December 2002 in the form of a Special Government Resolution. The resolution mandated the creation of a committee chaired by the head of the National Security Council and staffed by representatives from the security community and government ministries. The resolution also assigned CIIP responsibility to the General Security Service (GSS), Israel’s internal security apparatus, via the National Information Security Authority (NISA) [3].

A Steering Committee was created with the goal of consolidating steps to protect Israel’s CII assets. The committee’s mandate was to drive the activities of the various CIIP actors and especially that of NISA. The committee meets on a regular basis to discuss threats and security solutions. It has the authority, along with NISA, to determine that a (public or private) company or sector is critical and, therefore, subject to the executive power of NISA [3].

NISA was in place within the GSS Protective Security Division long before the Special Government Resolution. It held the responsibility for information security within the Israeli government, embassies and government-owned companies. NISA’s new executive powers came with substantial increases in human and budgetary resources, but its powers are limited — the IDF and Mossad are responsible for protecting their own information infrastructures and Director of Security of the Defense Establishment (“MALMAB”) is responsible for protecting the information infrastructures of the Ministry of Defense and the defense industrial base.

The Steering Committee and NISA initiated a process to define critical infrastructures and establish the legal framework that would allow them to assume their authority [3]. The Regulation of Security in Public Bodies Law of 1988 that sets out security requirements for public bodies and institutions was amended to reflect the new CIIP theme and to establish the authority given to NISA [8,9]. Despite its name, this law regulates public as well as private entities. The law provides NISA with very broad regulatory authority, including the power to determine if an infrastructure is critical; the power to approve the appointment of an officer in charge of securing vital information systems within a critical infrastructure; the power to give directions and instructions to the officer regarding required security actions, including control and reporting; and the power to inspect and audit the state of CIIP within a
regulated entity. Put simply, the law represents a very central-ist and hierarchical approach towards CIIP, one that provides almost no discretion to the regulated entities, including those that are privately-held. Note that in order to address privatization processes in the Israeli economy, the Governmental Companies Law was amended to reflect the need to control security matters (including cyber security) in privatized companies [8,9].

3.3. Comparison of American and Israeli policies

Clearly, the American policy is at the right-hand side of the regulatory continuum whereas the Israeli policy is at the left-hand side of the continuum. This is very interesting because both countries see themselves as susceptible to external threats. The next section discusses why the two countries conceive CIIP differently despite the similarity with which they perceive the threat.

4. How should CIIP be perceived?

The comparative analysis reveals that the way in which states conceptualize CIIP and the emphasis they attach to one or more values in the conceptualization are of great importance in choosing regulatory arrangements. Clearly, the design of institutions is not value neutral and, hence, institutional choices reflect the values and conceptions states adopt to CIIP. Nevertheless, the efforts made thus far in conceptualizing CIIP have been insufficient, especially in capturing the values that influence national policy.

This section attempts to analyze CIIP conceptions and identify the values that underlie them. The analysis draws on models of the criminal process offered by Packer [16] and Roach [19], and proceeds to review a recent attempt by Abele-Wigert [1] to conceptualize CIIP perspectives. Abele-Wigert offers four perspectives for CIIP: a technical/system perspective, business continuity perspective, law enforcement perspective and national security perspective. Her analysis is very useful for describing policies in terms of the levels of operation and involved actors, but it does not consider the values that influence the choices made by governing institutions. However, Abele-Wigert’s conceptions of business continuity and national security can be used as bases for models that explain the policies chosen by states. Indeed, by adopting the conceptions of business continuity and national security as models for CIIP, and discussing the values underlying institutional choices taken by governments (neo-liberal economic efficiency values and security values), a conceptualization is presented that better explains institutional choices.

The importance of injecting values into the discourse of CIIP models cannot be understated. The American and Israeli institutional choices in governing CIIP show how different value systems are reflected in the adoption of almost opposing systems, and how competition between these sets of values results in movement along the regulatory continuum.

4.1. Why build models?

Why would one want to build CIIP models? What roles would these models play? To answer these questions, we draw on seminal work related to models of the criminal process. Packer [16] framed two models of the criminal process, the crime control model and the due process model. He discussed the competition (“antinomy”) between the value systems that underlie these models, the regulation of criminal conduct and the rights of the individual, respectively. Roach [19] added two additional models, reflecting values that were less significant (or less known) during Packer’s era. While these works deal with the criminal process (and in general with criminal justice), they elucidate the role that models play in explaining the operation of processes and policies, in terms of is and ought, as well as in pointing out the competition between the values that support the models, and the adjustments between the competing demands of the value systems.

Roach observes that models are helpful in three ways, two of them normative and the third positive. First, models enable one to “judge the actual or positive operation of a system”. They provide tools to locate, criticize and correct a policy or system relative to the model, and to describe how a complex system may contain elements of different models. Second, models “provide a normative guide to what values ought to influence the system”. Different models are based on different, possibly conflicting, values. In the criminal process, the two competing values are the regulation of criminal conduct and the rights of the individual. By comparing models and deciding between them, we take a normative stand as to which values ought to be implemented. This is closely related to the first point, since any judging of a system or policy is largely dependent on the values that are found to be adequate for the system. Third and last, models play a positive, descriptive role in describing the “ideologies and discourses that surround” the system or policy. Here, the focus is on explanation and description. The models explain why a certain policy is in place through the analysis of the ideologies and discourses that affect it.

To conclude, models play positive and normative roles in analyzing existing policies, both explaining them and criticizing them. Note that Packer did not originally plan for the models to be “taken as Is and Ought” [16], but rather as tools that “represent an attempt to abstract two separate value systems that compete for priority in the operation of the criminal process. Neither is presented as either corresponding to reality or representing the ideal to the exclusion of the other” [16]. Nevertheless, models could, and should sometimes, be used as a basis for deciding on an ideal policy or process and, as Roach suggests, play an important normative role. For this reason, CIIP policies must also be analyzed through models.

4.2. Prior attempts at modeling CIIP

Despite the interest in CIIP, relatively little research has focused on understanding CIIP national policies and the differences between them. One exception is the work of Dunn and Abele-Wigert [1,6], which describes CIIP policies in more than twenty countries. Abele-Wigert, in particular,
uses empirical information about policies to frame them in a variety of perspectives. While arguing that most countries perceive CIIP as a national security issue, she indicates that CIIP can be conceptualized in terms of four perspectives: the system level/technical perspective, business continuity perspective, law enforcement perspective and national security perspective. She argues that these perspectives differ in two dimensions. The first dimension is the level of operation (technical, legislative, organizational and international); the second relates to the actors involved in protection efforts.

The system level/technical perspective approaches CIIP as a matter of “IT-security or information assurance” addressed by “technical means” such as firewalls, anti-virus software and intrusion detection software [1]. CIIP is addressed at the tactical/micro level by information security and information systems professionals who use technical tools to achieve information security.

According to Abele-Wigert, the business perspective views a firm's information infrastructure as an essential part of the business process. Its failure entails an adverse effect on business continuity. She acknowledges that “the means of achieving this [business process availability] coincide, by and large, with the ideas of the technical community” [1], but she distinguishes between the two because the business perspective focuses on organizational and human aspects in addition to technical aspects. In other words, the protection of a firm's cyber assets is dealt with by management; it involves the creation of a company policy, management leadership, etc., on top of the technical process. We add one more distinction related to the actors involved in protection efforts because the business perspective requires the designation of corporate officers (CIOs and CISOs) as responsible for protecting their firm’s information infrastructures. The inclusion of management controls in the NERC Critical Infrastructure Protection Cyber Security Standard is an example of such involvement.

The law enforcement perspective views CIIP as an aspect of cyber crime, together with computer hacking and fraud, Internet child pornography, phishing, and other computer security breaches. The perspective provides that CIIP should be addressed through traditional law enforcement mechanisms, i.e., by deterring legislation, post factum legal action and international cooperation.

The fourth perspective is the national security perspective where states acknowledge the potential damage that cyber attacks can cause. Hence, it is perceived as a threat to security, possibly survival. According to Abele-Wigert, this results in the involvement of actors from the public sector (including the security apparatus) and the private sector; as well as in operations at various levels (technical, legislative, organizational and international levels). Table 1 summarizes the differences between the various perspectives.

Abele-Wigert argues that the four perspectives are distinguished by two factors — the levels of operation taken to address CIIP and the actors involved. Her attempt at conceptualizing CIIP is, thus, very useful in describing CIIP policies worldwide.

The main drawback of Abele-Wigert’s analysis is that it does not consider the values that underlie the perspectives. Thus, her work cannot explain how competing or contrasting values affect the choices made by governments. The American and Israeli CIIP policies both reflect a national security perspective and both involve actions at various levels by various actors. However, having analyzed these policies and seen the differences between them, a pressing question remains: How is it that American and Israeli policies – which reflect identical conceptions of CIIP – are so different from each other? This example leads us to believe that new models, perhaps based on Abele-Wigert’s four perspectives, but supplemented by additional normative analysis and injected with values, need to be developed.

The reason for the inability of the four perspectives to distinguish between the opposing American and Israeli policies is because these perspectives, in Packer’s words, do not rise above the “welter of more or less connected details that make up an accurate description of the myriad ways in which the... process does operate or may be likely to operate” [16]. These perspectives tell us how the systems operate and who is involved. But they do not provide a normative model (or models) that “let(s) us perceive the normative antinomy that runs deep in the system,” and between systems. A good normative model would require attention to the values that underlie the policies and to political ideology and, thus, help address and explain the differences within and between systems.

### 4.3. From perspectives to models

Despite their drawbacks, some of the perspectives proposed by Dunn and Abele-Wigert offer good starting points for abstract models that can capture the ideology that underlies the policies taken by governments to address CIIP. This is true so long as it is possible to attach values to them and ensure that they can serve the positive and normative purposes outlined by Roach. Of the four perspectives, two are very attractive — the business model and the national security model. However, it is first necessary to discuss the technical/system and law enforcement perspectives, and eliminate them as candidates.
Classifying CIIP as a technical matter is quite rare, and for good reason. Both the public and private sectors understand that security breaches entail adverse consequences beyond the technical level. Corporate officers and directors of firms that operate critical infrastructures as well as firms in the broader business environment recognize the importance of information security to ensure business continuity and maintain their firms’ reputation and bottom lines. Information security policies are no longer left to the discretion of technical personnel such as system administrators or computer engineers. Information security matters are now part of the management processes controlled by CIOs and CISOs. Nevertheless, the technical perspective is still viable; it explains why (highly technical) CERT teams are part of CIIP policies. But perhaps more important than the rarity of the technical perspective, focusing on the technical level, which is not based on any value, is clearly of no use in understanding how political differences result in different policies.

The law enforcement perspective, on the other hand, does have an underlying value — the regulation of criminal conduct that underlies Packer’s crime control model. This seems quite plausible at first, as attacking a CII can be categorized as criminal activity. In other words, a hacker is a hacker, whether she hacks into a bank system to cripple it or whether she does it to steal money.

However, I argue that there are two points that make cyber attacks on CIs different from other forms of cyber crime. First, the relevant actors act on different motives. Cyber criminals live off our economies. A Russian crime syndicate has no incentive to destroy a bank’s information systems because it uses them as a tool to maximize its profits (unless it is paid to do it by an entity with other motives). Nation states and terrorist organizations, on the other hand, have different objectives — to spy on or to cripple or destroy the targeted information infrastructure. The two different objectives require different protective policies.

The second point applies specifically to information warfare conducted by nation states. Enemy soldiers who participate in warfare come under the purview of special laws of war, not criminal law. By the same token, designating and dealing with information operations against critical infrastructure assets as cyber crime is problematic. Also, policies that address cyber crime (and the values that underlie them) are usually focused on the post factum punishment for crimes. While the punishment of individuals, who damage or attempt to damage critical infrastructures, is important and entails a deterring effect, the main focus of CIIP is protective and defensive, seeking to prevent an attack ex ante through protective means. Thus, a perspective that looks to punish rather than prevent is not appropriate in the context of this work.

This leaves two candidates: the business continuity perspective and the national security perspective. While the two perspectives share a common characteristic, which is the importance they attach to the continued, uninterrupted availability and functionality of CIs, they seem to be based on competing values — neo-liberal economic efficiency values on the one hand and safety and security values on the other. This conflict is elaborated below.

The demise of the system level perspective has led to the widespread acceptance of the business continuity perspective. The business perspective considers the incentives of firms that manage and control critical infrastructures. Information security is a business management issue viewed in terms of return-on-investment and risk management. Put differently, this perspective seeks to advocate a business case for investing in information security by incorporating this matter into management processes. The underlying idea is that a private firm has an incentive to ensure that goods are produced or provided as it attempts to maximize profits. Security, in other words, is a cost in the economic equation of costs and benefits. Assuming that one could build a strong business case for information security in terms of return-on-investment makes the business perspective very plausible.

The discussion above also implies that a value based on the ideals of neo-liberal economics can be attached to the business perspective. This is very important in market economies that are founded on the notion that individuals (and firms) should be free to make choices based on their preferences. It is assumed that such choices, involving tradeoffs in resource allocation, will be optimal and efficient. In the case of CIIP, asset owners and operators would be left alone to decide about protection policies because it is assumed that the goal of business continuity (and, by extension, profitability) induce them to take responsible decisions. The presence of a value underlying this perspective suggests that it may serve as a CIIP model.

The national security perspective is perhaps the most straightforward candidate for a CIIP model. It is based on the important values of security and public safety, which every state endorses. It is also straightforward because of the nature of the threat against which CIs should be protected. The threat emanates from adversaries, mainly nation states and terrorist organizations, who have the intent, resources and capabilities to carry out attacks on critical infrastructure assets.

4.4. Value conflicts and models

As mentioned above, a conflict exists between the values underlying the business continuity and national security models — the values attached to the market and the values of safety and security. In fact, a business entity would have incentives (without government regulation) to apply stricter security measures in two cases: (i) if there is a clear return on security investment, and (ii) the mitigation of costs associated with risks is clear enough (and cost-effective). In such cases, the market mechanism could lead private entities to make investments in adequate levels of security. However, this is usually not the case, mainly because it is very hard to show a return on a security investment and/or private firms do not have adequate incentives due to market failures [2,7].

The interests may align in certain extreme cases. In wartime, for example, the profit-maximization tendency of firms coincides with the government’s desire for increased production to support military operations. Increased production by private firms may be perceived as supporting the military in a time of crisis while it actually represents profit-maximization and self-interest. This example, however, does
not represent the general relationship between safety and security values and neo-liberal economic efficiency values. On the contrary, these values may easily come into conflict with one another. In fact, as the American and Israeli approaches suggest, the models seem quite polarized. Indeed, the actual policies may involve a mixture of elements from both models, but it would still be useful to consider the polarized models as reference points for analysis.

The increased value of security in our society (partly due to a risk averse culture) is an excellent example of the polarity or tension between security and efficiency values [18]. Since the September 11, 2001 attacks and the Madrid and London bombings in 2004 and 2005, respectively, national and (especially) homeland security are at the forefront of domestic and foreign politics around the world. There are numerous indications of this development such as domestic legislation related to counterterrorism, heightened international cooperation, and so on. As Lewis [11] has correctly observed, “One of the hallmarks of homeland security analysis in the United States is a willingness to adopt an exceptionally risk-averse approach to potential threats. Bureaucracies tend to be inherently risk averse and the events of September 11 increased this tendency”. This has resulted in the willingness to heighten the value of security over that of economic efficiency.

The new regulatory mechanisms introduced to govern CIIP in the chemical and energy sectors in the US are probably due to such a shift in values. The movement along the regulatory continuum from Points F/G in Fig. 1 (voluntary self-regulation/market mechanism) to Point E (enforced self-regulation) represents the tension between the two values, and more specifically, adjustments between the competing demands of these value systems. The higher intervention by government (through approval and oversight) is a move towards more prescriptive attitude in two sectors that are considered to be inherently risky. If the United States were to adopt similar regulatory arrangements in other critical infrastructures, it would imply that the value of security has gained strength relative to economic values.

Another interesting example is that of the Committee on Foreign Investment in the United States (CFIUS), which determines if foreign investment in a US firm threatens national security. CFIUS is an interagency committee chaired by the Department of the Treasury and staffed by representatives from various departments, including the security community. Traditionally, the United States has welcomed foreign investment as part of its open market economic ideology, and CFIUS has rarely restricted foreign direct investment (FDI). However, in 2003, President Bush added the Department of Homeland Security to CFIUS, “shifting the committee’s balance of power significantly in favor of agencies prioritizing security over economic policy considerations” [10].

But this was only the first step. In July 2007, Congress enacted the Foreign Investment and National Security Act of 2007 (FINSA), which emphasized security at the expense of economic needs. FINSA introduced the notions of critical infrastructure and homeland security into the CFIUS review process. Also, it requires CFIUS to conduct investigations when foreign investment transactions are initiated by foreign government-owned or -controlled entities. Previously, in these kinds of transactions, the burden of proof was on CFIUS to show that a particular transaction was a threat to national security. The new requirements have shifted the burden of proof to the investing entity, which has to show that it is not a security threat. Thus, the presumption that FDI contributes positively to the US economy has been replaced by one that FDI could pose a threat to national security and, therefore, requires heightened scrutiny.

The security preference has resulted “in more investigations and stricter security-related conditions for CFIUS approval” [10]. Furthermore, following the recent Dubai Ports World affair, numerous attempts have been made to reform the Exon-Florio Amendment, including moving the CFIUS Chairmanship from the Department of the Treasury to the Department of Defense or the Department of Homeland Security. Although these attempts have been unsuccessful, they point to the shift in priorities within the US Government and Congress from neo-liberal economic values towards national security.

The growing prioritization of security and the risk averse mindset are closely related to the idea of the “safety state” developed by Raab [18]. Raab argues that we are witnessing “the elevation of safety as the paramount value in the lives of states and of persons”. In other words, there has been an increase in the value of security relative to other values, including neo-liberal economic values. Indeed, it is not yet clear that security is the paramount value in our society (or FINSA would have been more strict), but its value is definitely on the rise relative to economic or welfare interpretations. Note that I do not categorize the migration to the “safety state” as good or bad. Rather, I wish to point out its existence and the fact that it has and will have implications on how the public and governments view national security versus economic values.

In Israel, by contrast, the national security value is still dominant relative to economic and other values. The predominance of security has contributed to relatively harsh command and control regulatory arrangements. Given the perceived threats, it is clear that Israel’s security-dominant policy will probably remain as such.

4.5. Relevance of model distinctions

The business continuity and national security models appear to share a common need for the uninterrupted availability and functionality of CIIs. If this is so, the question is: What is the relevance of a normative determination of CIIP as a matter of business continuity or as a matter of national security? Simply put, why is it important?

There are three answers to this question. The first, and most obvious, is that a common language is needed to discuss this issue within and between government, the private sector and academia; otherwise, the understanding of the concept of CIIP is limited at best.

The second is consequential — with implications regarding the choice of institutional arrangements for addressing CIIP. A business continuity model might suggest that firms operating critical infrastructure assets should be left to address the information warfare threat on their own. On the
other hand, a national security model would suggest that government has a substantial role in assuring adequate levels of CIIP. Ascribing CII threats to national security is relevant to any analysis that attempts to understand the roles that institutions play in CIIP. As one might fairly assume, this serves as a focal point for analyzing government intervention (or the need for intervention) in order to ensure optimal levels of CIIP.

The third answer, which is related to the second, deals with the identification of the good in question. The view of CIIP as a business continuity issue implies that information security is a component in the production of critical infrastructure goods and services. However, the view of CIIP as a national security issue implies that it is a component of the (very important) national security good. This dichotomy is the result of the dual nature of a CIIP good or service. From a private firm’s perspective, the security of its information systems is a component in the production cycle of a unit or service—a Watt of electricity, a bank service, a barrel of crude, and so on. Every decision regarding it is, therefore, a regular business decision taken by a producer or provider. From the state’s perspective, in its role as the guardian of its citizens, CIIP is an essential component of national security. National security comprises many components, including physical security, border security, economic security and CI security. It is a public good that is commonly and usually provided by the state. In fact, national security is a classic example of a public good [20]. Therefore, depending on the perspective or model adopted, CIIP can be analyzed in multiple ways.

CIIP’s dual nature has additional implications when analyzing government CIIP policies. For example, if CIIP is viewed as a component of national security, then a policy that endorses a hands-off approach can be seen as a decision to contract out or privatize an important element of national security. This policy can then be examined using the lenses of privatization and outsourcing theories.

5. Conclusions

With the exception of Dunn’s work, the socio-political dimensions of CIIP have been largely ignored. But these dimensions are critical to understanding CIIP policies. This paper has proposed a different way of viewing CIIP. Specifically, it has sought to model CIIP as an instrument that would better explain national regulatory policies. It has shown that such policies are the result of the antinomy between competing sets of values—security and economic efficiency. The strength of one value relative to the other determines which regulatory approach is chosen. Our future research will investigate normative issues, helping identify the model and values that ought to be selected. This will provide insights into whether one model should prevail over the other, and whether governments should opt for one model over another when crafting national policies related to CIIP.

References

